Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

Claims 1-36 (Cancelled)

37. (New) A method for enabling an image to be authenticated, the method comprising:

providing a digital signature associated with a device;

allowing a user to capture the image utilizing the device;

hashing a file containing both the captured image and the digital signature associated with the device to produce a digest; and

encrypting the digest using a private/public key pair associated with the user to create a digital signature for the user.

38. (New) The method of claim 37, wherein the device is capable of electronically transmitting images.

39. (New) The method of claim 37, wherein the device comprises a digital camera.

40. (New) The method of claim 37, wherein the private/public key pair associated with the user is provided to the device via a radio frequency interface or a smart card.

41. (New) The method of claim 40, wherein the radio frequency interface or the smart card further provides information relating to the user to the device.

42. (New) The method of claim 41, wherein information relating to the user comprises an identification of the user.

43. (New) The method of claim 40, further comprising:

equipping the device with a disabling mechanism;

detecting whether the user is an approved user; and

disabling the device when the user is not an approved user.

44. (New) The method of claim 43, wherein the device detects whether the user is an approved user via the radio frequency interface or the smart card.

45. (New) The method of claim 40, wherein the radio frequency interface or the smart card further provides a public key associated with an owner or an intended owner of the captured image to the device.

46. (New) The method of claim 45, further comprising:

encrypting the captured image using the public key associated with the owner or the intended owner of the captured image.

47. (New) The method of claim 37, wherein the file containing both the captured image and the digital signature associated with the device is stored in a memory of the device.

48. (New) A system for enabling an image to be authenticated, the system comprising:

means for providing a digital signature associated with a device;

means for allowing a user to capture the image utilizing the device;

means for hashing a file containing both the captured image and the digital signature associated with the device to produce a digest; and

means for encrypting the digest using a private/public key pair associated with the user to create a digital signature for the user.

49. (New) The system of claim 48, wherein the device is capable of electronically transmitting images.

50. (New) The system of claim 48, wherein the device comprises a digital camera.

51. (New) The system of claim 48, wherein the private/public key pair associated with the user is provided to the device via a radio frequency interface or a smart card.

52. (New) The system of claim 51, wherein the radio frequency interface or the smart card further provides information relating to the user to the device.

53. (New) The system of claim 52, wherein information relating to the user comprises an identification of the user.

54. (New) The system of claim 51, further comprising:

means for equipping the device with a disabling mechanism;

means for detecting whether the user is an approved user; and

means for disabling the device when the user is not an approved user.

55. (New) The system of claim 54, wherein the device detects whether the user is an approved user via the radio frequency interface or the smart card.

56. (New) The system of claim 51, wherein the radio frequency interface or the smart card further provides a public key associated with an owner or an intended owner of the captured image to the device.

57. (New) The system of claim 56, further comprising:

means for encrypting the captured image using the public key associated with the owner or the intended owner of the captured image.

58. (New) The system of claim 48, wherein the file containing both the captured image and the digital signature associated with the device is stored in a memory of the device.

59. (New) A computer readable medium containing a computer program for enabling an image to be authenticated, the computer program comprising program instructions for:

providing a digital signature associated with a device;

allowing a user to capture the image utilizing the device;

hashing a file containing both the captured image and the digital signature associated with the device to produce a digest; and

encrypting the digest using a private/public key pair associated with the user to create a digital signature for the user.

60. (New) The computer readable medium of claim 59, wherein the device is capable of electronically transmitting images.

61. (New) The computer readable medium of claim 59, wherein the device comprises a digital camera.

62. (New) The computer readable medium of claim 59, wherein the private/public key pair associated with the user is provided to the device via a radio frequency interface or a smart card.

63. (New) The computer readable medium of claim 62, wherein the radio frequency interface or the smart card further provides information relating to the user to the device.

64. (New) The computer readable medium of claim 63, wherein information relating to the user comprises an identification of the user.

65. (New) The computer readable medium of claim 62, wherein the computer program further comprises program instructions for:

equipping the device with a disabling mechanism;

detecting whether the user is an approved user; and

disabling the device when the user is not an approved user.

66. (New) The computer readable medium of claim 65, wherein the device detects whether the user is an approved user via the radio frequency interface or the smart card.

67. (New) The computer readable medium of claim 62, wherein the radio frequency interface or the smart card further provides a public key associated with an owner or an intended owner of the captured image to the device.

68. (New) The computer readable medium of claim 67, wherein the computer program further comprises program instructions for:

encrypting the captured image using the public key associated with the owner or the intended owner of the captured image.

69. (New) The computer readable medium of claim 59, wherein the file containing both the captured image and the digital signature associated with the device is stored in a memory of the device.